

May 15, 1998

Page 2

specific technical requirements by law enforcement is a source of delay and continues to frustrate the efforts of the Subcommittee. The Subcommittee's schedule has already slipped by at least a month and will continue to do so without substantive input from law enforcement.

Consequently, the Subcommittee formally requests that law enforcement do the following to advance the ESS process and clarify its surveillance requirements:

1. Propose language for baseline text which details law enforcement's enhanced surveillance requirements;
2. Designate or provide reference documents specifically describing, in sufficient technical detail, the appropriate enhanced surveillance requirements (e.g., ESI, Colgate Letter, FCC Petition); and
3. Review and respond affirmatively to the attached contributions which identify issues and areas of uncertainty regarding law enforcement's enhanced surveillance requirements. To the extent they exist, the Subcommittee also requests that law enforcement address the documents' common elements and respond in a comprehensive manner accordingly.

Furthermore, we ask that you provide the requested feedback by the Subcommittee's next meeting scheduled in Toronto on June 16-17, 1998. The Subcommittee will continue to send requests for input and clarifications by law enforcement as the need arises in order to facilitate the ESS process. Your good faith participation is necessary to ensure the success of this project.

We look forward to your input. If you have any questions, please contact me immediately.

Best Regards,

Peter Musgrove
Chair, TIA Subcommittee TR45.2 ESS Ad Hoc Group

May 15, 1998

Page 3

PM:jm

cc: Janet Reno, U.S. Attorney General
Subcommittee TR45.2 Members
Wayne Zeuch, T1S1 Chair
Asok Chatterjee, T1P1 Chair
John McDonough, T1M1 Chair

Enclosures

Synacom Technology, Inc. (reviewed and modified)
Siemens Telecom Networks (as presented)
NORTEL (as presented)
Lucent Technologies (as presented)

Telecommunication Industry Association
Ad Hoc on Enhanced (Lawfully Authorized Electronic) Surveillance Services
Marriott Reach Resort
Key West, FL USA
May 6, 1998

Punch List (Rev. 5)

Contact:

Kirk Carlson
Synacom Technology, Inc.
3031 Tisch Way Suite 400
San Jose, CA 95128
Phone: (+1) (408) 296.0303
Fax: (+1) (408) 296.0982
e-Mail: kirk@synacom.com

Under contract to the CTIA

Abstract:

This document tracks the basic punch list items as being requested and clarified by law enforcement. This version includes items requested by the FBI CIS and other issues that have reached consensus in the group.

Recommendations:

Liaison this to the FBI CIS to get their positive written confirmation that this is a complete and accurate assessment of the technical capabilities that they are seeking beyond CALEA and J-STD-025.

Notice:

The contributor grants a free, irrevocable license to the Telecommunications Industry Association (TIA) to incorporate text contained in this contribution and any modification thereof in the creation of TIA standards publication; to copyright in the TIA's name any TIA standards publication even though it may include portions of this contribution; and at TIA's sole discretion to permit others to reproduce in whole or in part the resulting TIA standards publication.

©1998 Synacom Technology, Inc. Permission is granted to TIA Committee participants to copy any portion of this document for legitimate purposes of the TIA. Copying for monetary gain or other non-TIA related purposes is prohibited.

This document has been prepared by Synacom Technology, Inc. to assist the TIA/EIA TR45.2 Subcommittee. It is intended for discussion purposes only. It may be amended or withdrawn at a later time and is not binding on any member of the TR45.2 Subcommittee, the CTIA, its members, or Synacom Technology, Inc.

Assumptions

The proposed functionality is to complement and enhance the lawful electronic surveillance capabilities

described in J-STD-025.

Normal text reflects law enforcement requirements. References in square brackets are to the Appendix 1 changes to §64.1708 within the DOJ-FBI Joint Petition to the FCC.

Italicized text shows comments and requirements that go beyond the law enforcement requirements. These comments were developed by the TIA TR45.2 Ad Hoc on Enhanced Electronic Surveillance.

Due to overlapping functionality, some call events may be redundantly reported. It is our understanding that law enforcement desires the redundancy to reveal *modus operandi* and other personality characteristics. However, there is no need to redundantly report signaling that is reported with other messages.

Punch List

The following services requested by law enforcement may serve as enhancements to the services defined in J-STD-025.

1. Content of Held Conference Calls

This capability corresponds to the DOJ¹ capability item entitled "Content of conferenced calls" or the DOJ-FBI joint petition capability item entitled "All Content of Conferenced Calls."

Monitor an intercept subject's multi-party service (e.g., conference calling) when two or more associates are allowed to converse when the intercept subject leaves the conversation temporarily or permanently. [(a)]

Monitor an intercept subject's multi-party service (e.g., meet me conference) when two or more associates are allowed to converse without the intercept subject's participation.

Call content shall not be delivered for a single party on hold. [(a)(2)]

¹From the February 3, 1998 letter from Steve Colgate, Assistant Attorney General, to Thomas Wheeler, President of CTIA

2. Dynamic Party Reporting

This capability corresponds to the DOJ capability item entitled "Party Hold, Party Join, Party Drop" or the DOJ-FBI joint petition capability item entitled "Party Hold, Party Join, and Party Drop Messages."

Report the identities of the parties to a multi-party conversation (e.g., three-way calling, call waiting, conference calling) when connections are allow to change to the extent known to the accessing switching system. [(b)]

Report the identities of the parties to a multi-party conversation (e.g., meet-me conference) when connections are allow to change to the extent known to the accessing switching system. [(b)(4)(iv)]

Report the identities of the parties to specialized multi-party conversations with unusual call control (e.g., barge in). [(b)(7)]

Report the identities of the parties to a two-party conversation when connections to parties are allowed to change (e.g., hold, retrieve, park, pickup) at all times to the extent known to the accessing switching system. Such reporting enables law enforcement to distinguish participation by the intercept subject in multiple simultaneous calls. [(b)(4)(i)]

We are requesting input as to whether the reporting mechanism should be stateless (self contained messages) or state driven (dependent upon prior transmitted information).

We are requesting input as to whether the reporting mechanism should be for the delivered CCC or the parties connected to a particular call (as identified with a call identifier).

This capability corresponds to the DOJ capability item entitled "Access to subject-initiated dialing and signaling" or the DOJ-FBI joint petition capability item entitled "Subject-Initiated Dialing and Signaling."

Report and identify intercept subject initiated signaling or feature keys used to invoke or control an individual subject's call control features (e.g., switchhook flash, hold key, flash key, transfer key, conference key, make busy key, stop hunt key) to the extent know to the accessing switching system and regardless of the use of outcome of the processing of that signaling. [(c)(1)]

Include the nature of number indicator and presentation restriction indicators with any calling, called or redirecting number delivered. [(c)(2)]

Report when the subject's phone goes off-hook and then on-hook without any dialed digits. [(c)(3)]

There is no need to report and identify intercept subject initiated manual signaling or feature keys used to invoke or control an individual subject's advanced business service call control features (e.g., CENTREX features, wireless office features) to the extent know to the accessing switching system and regardless of the use of outcome of the processing of that signaling.

There is no need to report and identify intercept subject initiated signaling used to invoke or control third party call control features (e.g., Q.932 REGISTER, FACILITY, and non-call associated RELEASE messages) to the extent known to the accessing switching system and regardless of the use or outcome of the processing of that signaling.

There no need to report and identify intercept subject voice activated signaling used to invoke or control features to the extent known to the accessing switching system and regardless of the use of outcome of the processing of that signaling beyond that reported in J-STD-025.

There is no need to report and identify all subject initialized signaling, especially when that signaling is not normally perceptible (e.g., terminal management signaling, mobility management signaling, power controls).

4. Network Signal Reporting

This capability corresponds to the DOJ capability item entitled "Notification Message (in-band and out-of-band signaling)" or the DOJ-FBI joint petition capability item entitled "Notification Messages for In-band and Out-of-band Signaling."

Report and identify out-of-band network signaling applied toward the intercept subject by the accessing system that would normally be heard or felt by the intercept subject (e.g., power alerting, out-of-band tone commands). [(d)(1)(A, B)]

Report and identify out-of-band network signaling applied toward the intercept subject that would normally be seen by the intercept subject (e.g., subject call status indicators). [(d)(1)(C)]

Detect and report any audible in-band tones indicating an incoming call applied by the accessing system (e.g., call waiting alert). [(d)(1)(B)]

Report any alphanumeric information which may be displayed to the intercept subject (e.g., calling party number, calling party name, redirecting party number, redirecting party name, display information element) associated with circuit-mode calls. Note that SMS or user-to-user information are information services not subject to intercept. [(d)(1)(D)]

Detect and report any audible in-band call progress tones applied by the accessing system toward the intercept subject (e.g., dial tone, busy, re-order, confirmation tone, denial tone, recall dial tone, audible alerting, special information tones (SIT)).

There is no need to report and identify out-of-band network signaling applied toward the associate that would normally be perceivable (i.e., heard, felt or seen) by the associate where such signaling cannot be derived through examination of the delivered call content (e.g., busy, audible alerting, call refused).

There is no need to report and identify network signaling to report information services such as the indicators of a Direct Station Select/Busy Lamp Field (DSS/BLF) or a message waiting indicator.

There is no need to report and identify in-band network signaling applied toward the associate at any time of the call (i.e., before or after cut-through).

5. Timing and Correlation

This capability corresponds to the DOJ capability item entitled "Timing to correlate call data and call content" or the DOJ-FBI joint petition capability item entitled "Timely Delivery of Call-identifying Information."

5a. Improved Correlation

Improve the correlation between the communications delivered over CCCs with the call-identifying information delivered over CDCs.

This may be implemented as one or more of the following:

- a. a non-unique number inserted into the CCC such as a dialed number for switched delivery or a burst of tones..
- b. synchronization of the CCC events and CDC messages.
- c. a unique identifier inserted into each content delivery that can be correlated with corresponding CDC messages. The insertion of such a marker may obscure call contents in violation of J-STD-025 or may require delay of call content delivery. [(e)(6)]
- d. systematic rotation through a group of CCCs.

5b. Contemporaneous Delivery

Call content shall be delivered contemporaneously with the call (i.e., with a delay of less than 2 seconds 98 percent of the time when the CCC or CDC is not congested or under flow control) at the point of demarcation.²

Call related events on the CDC shall be delivered contemporaneously (i.e., with a delay of less than 3 seconds 98 percent of the time when the CDC is not congested or under flow control) at the point of demarcation. [(e)(3)]

Non-call related events (e.g., ServingSystem messages, feature status reports and surveillance status report) on the CDC shall be delivered contemporaneously (i.e., with a delay of less than 5 seconds 98 percent of the time when the CDC is not congested or under flow control) at the point of demarcation. [(e)(5)]

5c. Synchronization of CCC and CDC

A marker shall be inserted into the CCC to mark the beginning of call content delivery. The insertion of such a marker

²This requirement nearly mandates the use of dedicated circuits for each intercept which in turn will raise the operational cost and complexity.

may obscure call contents in violation of J-STD-025 or may require delay of call content delivery. [(e)(2)]

The time stamp in the CCOpen message shall be within 100 ms of the time call content delivery begins referenced to the accessing system clock. [(e)(2)]

Events reported on the CDC shall be delivered within 3 seconds of the corresponding CCC delivery at the point of demarcation.

Is it acceptable to obscure call content to insert a marker or numeric tag (in violation of J-STD-025)?

Is it acceptable to delay call content to insert a marker or numeric tag (in violation of 5b above)?

5d. Accuracy of Time Stamps

All time stamps reporting a particular event should be within 100 ms for any particular system. [(e)(1)]

There is no need to synchronize time stamps to Coordinated Universal Time (UTC) to allow correlation of an event between various systems.

There is no need to define each event precisely, so that the time reported for an event is consistent between manufacturers.

May 15, 1998

Enhanced Surveillance Services (Rev. 5)

6. Surveillance Status Reporting

This capability corresponds to the DOJ capability item entitled "Surveillance Status Message" or the DOJ-FBI joint petition capability item entitled "Surveillance Status Message."

Report the activation, or deactivation of any individual surveillance. [(f)(1)]

Report the modification of any individual surveillance where such modification is relevant to a particular court order (e.g., CCC assignments, expiration date and time). [(f)(1)]

Periodically ensure each active CDC is operational. [(f)(2)]

Periodically report the active surveillances for each CDC [(f)(2)]

The period shall not be less than an hour nor greater than twenty-four hours. [(f)]

Report the CCCs assigned or de-assigned to individual surveillances. [(f)(3)]

The surveillances shall aggregate the status from the constituent IAPs required for a particular surveillance, such that a surveillance is considered active when all of the constituent IAPs are active and accessible.

The surveillances shall aggregate the status from the constituent IAPs required for a particular surveillance, such that a surveillance is considered degraded when at least one, but not all, of the constituent IAPs are active and accessible.

The surveillances shall aggregate the status from the constituent IAPs required for a particular surveillance, such that a surveillance is considered inactive when all of the constituent IAPs are inactive or inaccessible.

There is no need to report the activation or deactivation of individual IAPs as they apply to each court order.

There is no need to periodically ensure that all IAPs required for a surveillance are operational and report to law enforcement.

There is no need to provide message integrity to ensure that the message has not been altered in transmission.

There is no need to provide message sender authentication to ensure the integrity of message sender identification.

Enhanced Surveillance Service (Rev. 5) May 15, 1998

There is no need to provide message accountability to detect loss or insertion of messages.

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20
- 21
- 22
- 23
- 24
- 25
- 26
- 27
- 28
- 29
- 30
- 31
- 32
- 33
- 34
- 35
- 36
- 37
- 38
- 39
- 40
- 41
- 42
- 43
- 44
- 45
- 46
- 47
- 48
- 49
- 50
- 51
- 52
- 53
- 54
- 55
- 56
- 57
- 58
- 59
- 60

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100

Report any change or modification to a subscriber profile that may affect law enforcement's ability to obtain surveillances as they occur and regardless of the source of the change (e.g., service order, administrative change, subscriber controlled feature, remote feature access, automatic time-of-day change). [(g)(1)]

- authorization, de-authorization, registration, de-registration, activation or de-activation of any call redirection feature (e.g., any variation call forwarding, single number service, call deflection); [(g)(2)(A)]
- authorization or de-authorization of features or services that require the use of more than one simultaneous content channel to monitor the subject's activities (e.g., call waiting, call forwarding, call hold, call transfer, voice mail); [(g)(2)(B)]
- temporary suspension and re-instatement of service; and [(g)(2)(C)]
- permanent de-authorization of service.

- registered redirect-to numbers (e.g., any variation of call forwarding, call deflection, one number service); [(g)(3)]
- the name of the affected feature.

- new service orders for unrelated directory numbers by the intercept subject;
- directory number changes;; [(g)(2)(C)]
- personal mobility authorization, de-authorization, or suspension;
- terminal mobility authorization, de-authorization, or suspension; and
- number portability changes.

Punch List

Enhanced Surveillance Service (Rev. 5) May 15, 1998

Enhanced Surveillance Service (Rev. 5) May 15, 1998

8. CCC Operational Assurance

This capability corresponds to the DOJ capability item entitled "Continuity Check" or the DOJ-FBI joint petition capability item entitled "Continuity Check."

Periodically or continuously ensure each active idle dedicated circuit-mode CCC is operational by injecting a signal that indicates call content is not being delivered. [(h)]

The period need not be less than an hour and the period shall not be greater than twenty-four hours.

There is no need to ensure each active dedicated circuit-mode CCC is correctly configured.

There is no need to ensure each active packet-mode CCC is correctly configured and operational.

There is no need to ensure each active switched circuit-mode CCC is correctly configured and operational.

9. Post Cut-through DTMF Digit Reporting

This capability corresponds to the DOJ capability item entitled "Post cut-through dialing and signaling" or the DOJ-FBI joint petition capability item entitled "Dialed Digit Extraction."

Detect and report any intercept subject dialed post cut-through in-band DTMF digits irrespective of the interpretation of those digits. [(i)]

10. Separated delivery of conference calls

This capability corresponds to a supposedly dropped DOJ capability item.

There is no need to provide separated delivery of individual parties to a conference call. This item remains because the DOJ asked for separated delivery in their petition to the FCC. This is in contradiction to public statements and a letter from The Attorney General stating that they would no longer pursue this issue.

11. Limited number of CDC and CCC delivery protocols

This capability corresponds to a supposedly dropped DOJ capability item even though it was requested in the Joint DOJ-FBI Petition to the FCC as "Ceiling Limit on Number of Interfaces." [(j)]

There is no need to provide a limited number of CDC and CCC delivery protocols. This item remains because the DOJ asked for separated delivery in their petition to the FCC. It is even in Appendix A of the Joint DOJ-FBI Petition to the FCC that the CIS/BAH has stated in our last meeting as being the "meat" of the petition. This is in contradiction to public statements and a letter from The Attorney General stating that they would no longer pursue this issue.

[illegible]

Enhanced Surveillance Service (Rev. 5) May 15, 1998

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20
- 21
- 22
- 23
- 24
- 25
- 26
- 27
- 28
- 29
- 30
- 31
- 32
- 33
- 34
- 35
- 36
- 37
- 38
- 39
- 40
- 41
- 42
- 43
- 44
- 45
- 46
- 47
- 48
- 49
- 50
- 51
- 52
- 53
- 54
- 55
- 56
- 57
- 58
- 59
- 60

TR45.2 Enhanced Surveillance Services (ESS) AdHoc Group
May 4, May 5, and May 6, 1998
Marriott Reach Resort, Key West, Florida

TITLE: Punch list items 2 (and 3, 4, 8) with respect to multi-party calls.

SOURCE:

Siemens Telecom Networks
900 Broken Sound Parkway
Boca Raton, Florida – 33487

<http://www.stn.siemens.com>

ABSTRACT:

The flow sequences for a large conference call from an intercept subject and for a call waiting scenario are presented.

These flows could be used at the meeting as working paper to discuss, understand, and define the scope of some of the punch list items. These flows mainly address the punch list items 2 along with 3, 4, and 8.

Contact:

Nagaraja Rao
EWSD Systems Engineering
Siemens Telecom Networks
900, Broken Sound Parkway
Boca Raton, Florida – 33487

Phone: 561 955 8906

Fax: 561 955 8593

Email: Nagaraja.Rao@stn.siemens.com

Recommendations:

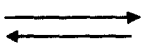
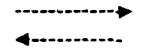

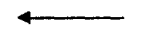





Walk-through the flows. Use the document as a working paper to analyze the requirements pertaining to the punch list items. Where appropriate, develop the text for the PN-4177 document to clarify the illustrated call sequences.

Notice:

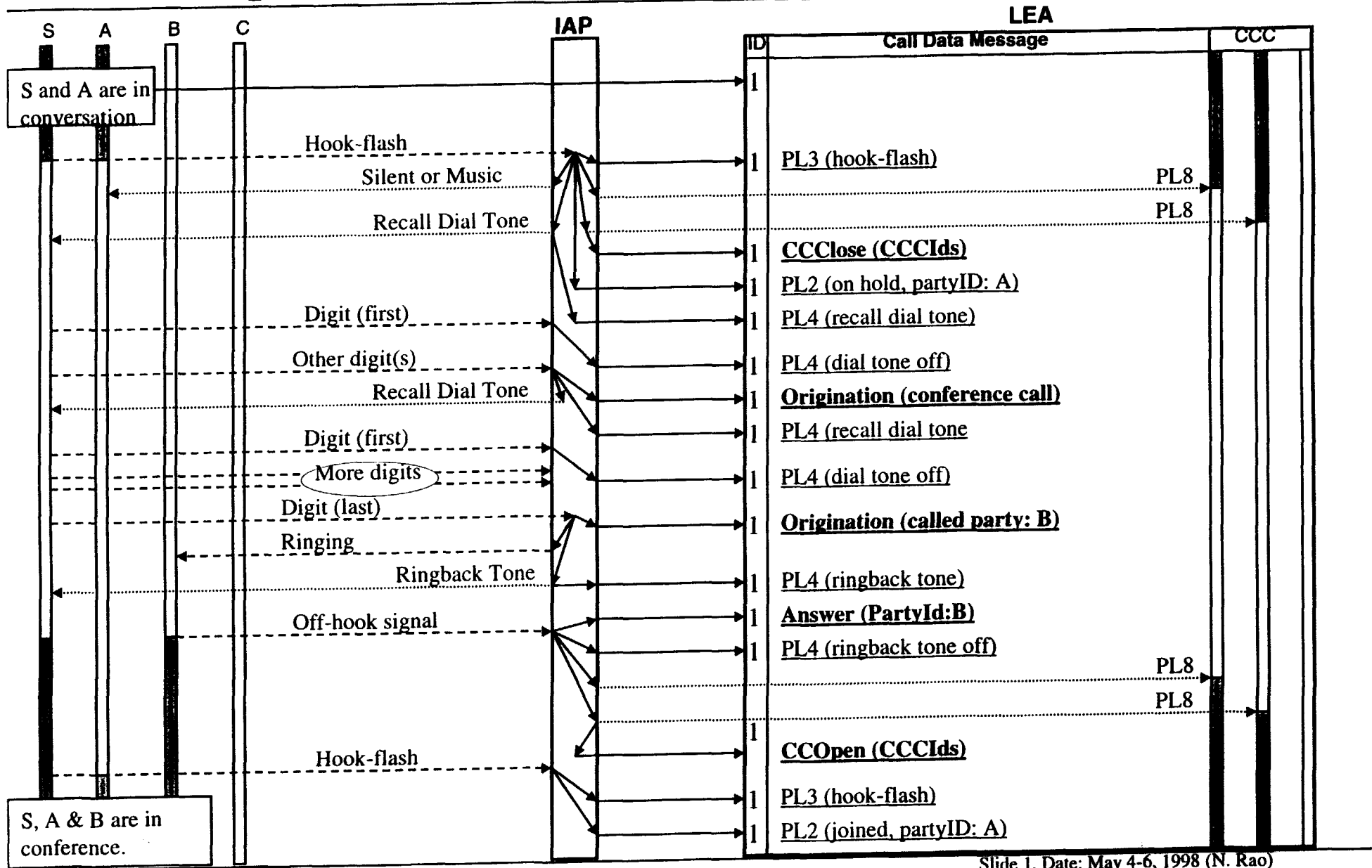
This document has been prepared by Siemens Telecom Networks to assist the TIA/EIA TR45.2 Subcommittee. It is intended for discussion purposes only. It may be amended or withdrawn at a later time and is not binding on any member of the TR45.2 Subcommittee or Siemens Telecom Networks.

Punch list items 2 and 3, 4, 8 with respect to multi-party calls.

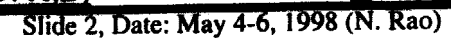
The following table helps to understand the flows:

Symbol	Description
	Message (a call data message to the LEA (e.g., ANSWER) or a D-channel message from/to an ISDN user (e.g., SETUP)
	Signal from/to the analog user (off-hook, hook-flash, ringing)
	Application or removal of tone to the LEA on the call content channel (e.g., C-Tone)
	Application a tone to the user (e.g., ringback tone)
	User A is on-hook
	User A is off-hook
	Subject S and User A are in communication with each other. .
	CCC without the call content.
	CCC with the call content.

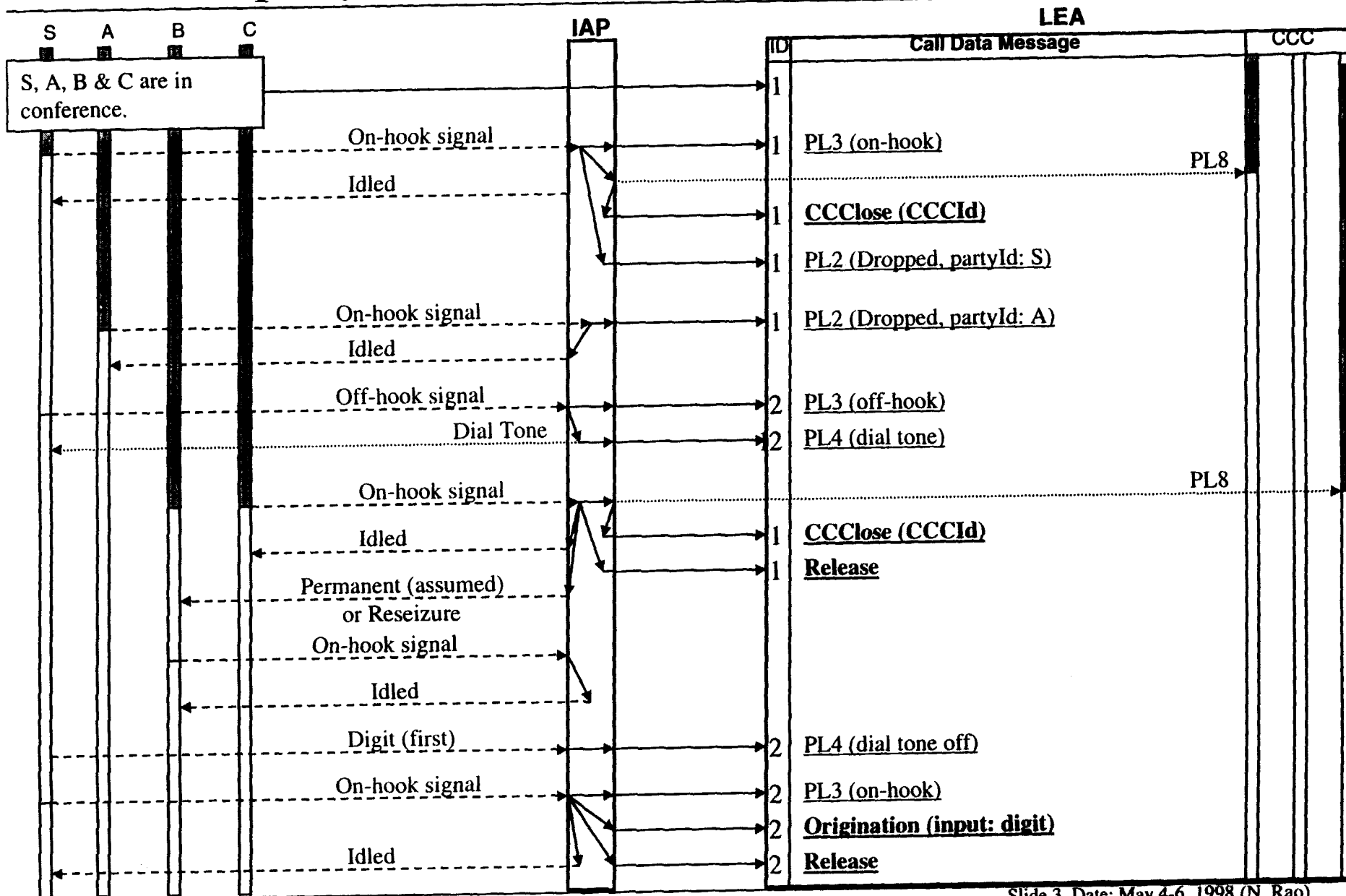
A multi-party conference calling + Transfer (analog) - 1/3



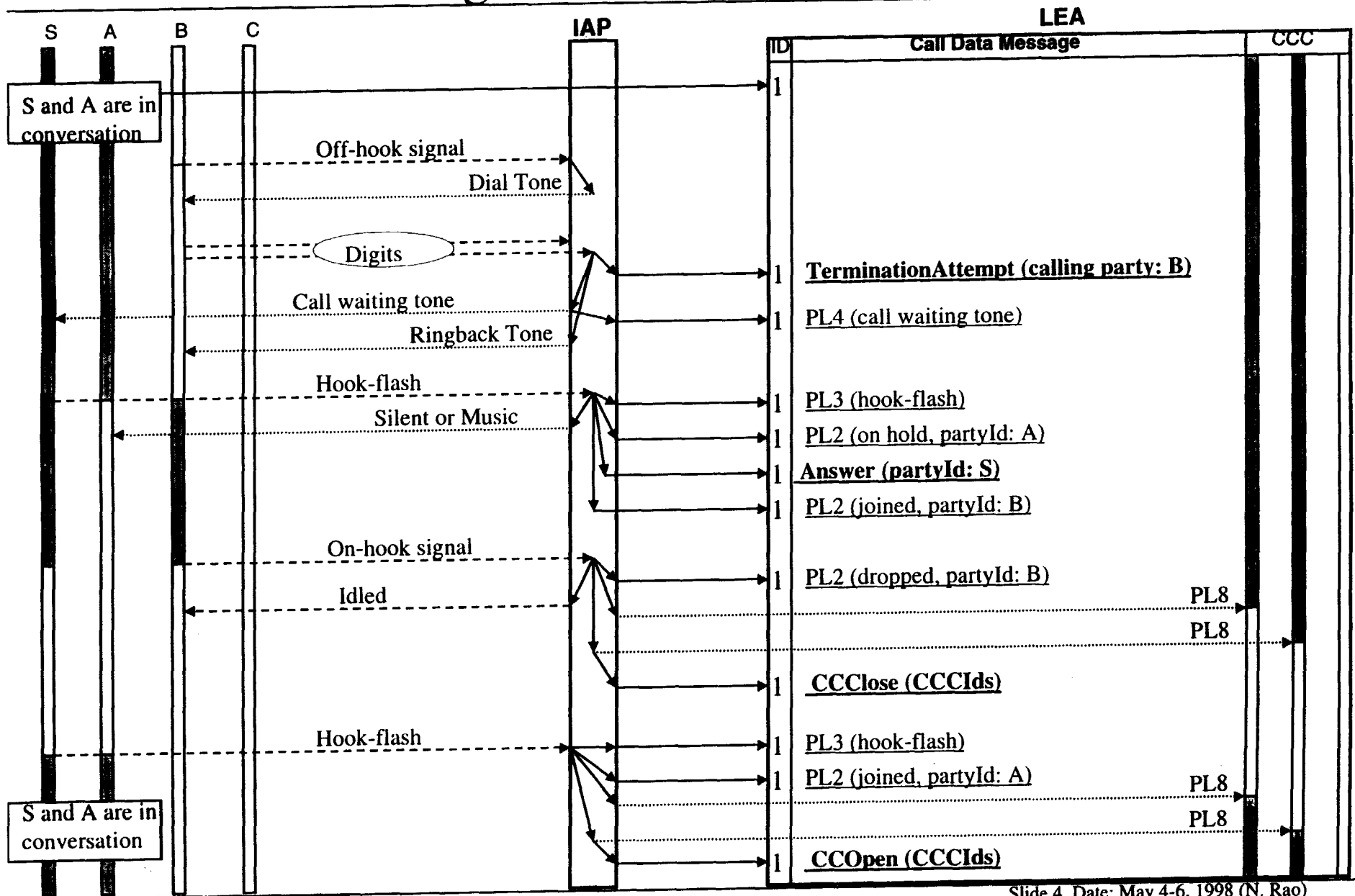
Siemens Telecom Networks



A multi-party conference calling + Transfer (analog) - 3/3



A call waiting scenario (analog)



TR45.2 Enhanced Surveillance Services (ESS) AdHoc Group
May 4, May 5, and May 6, 1998
Marriott Reach Resort, Key West, Florida

TITLE: Punch list items 3, 4, 8 with respect to Terminating calls.

SOURCE:

Siemens Telecom Networks
900 Broken Sound Parkway
Boca Raton, Florida – 33487

<http://www.stn.siemens.com>

ABSTRACT:

The flow sequences for calls terminating to the intercept subject are presented – intraoffice calls to an analog and to an ISDN user.

These flows could be used at the meeting as working paper to discuss, understand, and define the scope of some of the punch list items. These flows mainly address the punch list items 3, 4, and 8.

Contact:

Nagaraja Rao
EWSD Systems Engineering
Siemens Telecom Networks
900, Broken Sound Parkway
Boca Raton, Florida – 33487

Phone: 561 955 8906
Fax: 561 955 8593
Email: Nagaraja.Rao@stn.siemens.com

Recommendations:

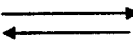
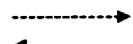
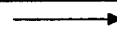
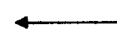





Walk-through the flows. Use the document as a working paper to analyze the requirements pertaining to the punch list items. Where appropriate, develop the text for the PN-4177 document to clarify the illustrated call sequences.

Notice:

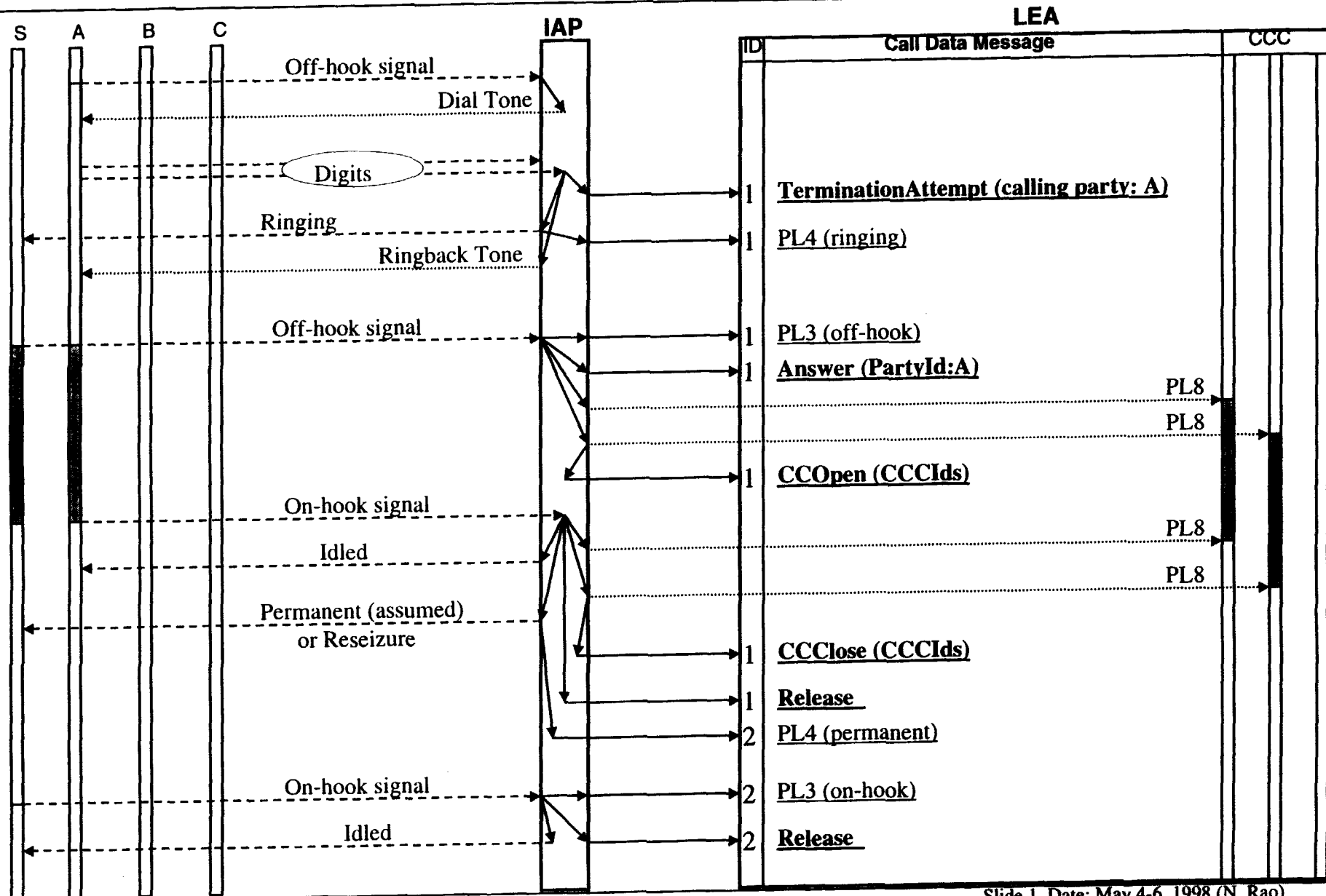
This document has been prepared by Siemens Telecom Networks to assist the TIA/EIA TR45.2 Subcommittee. It is intended for discussion purposes only. It may be amended or withdrawn at a later time and is not binding on any member of the TR45.2 Subcommittee or Siemens Telecom Networks.

Punch list items 3, 4, 8 with respect to Terminating calls.

The following table helps to understand the flows:

Symbol	Description
	Message (a call data message to the LEA (e.g., ANSWER) or a D-channel message from/to an ISDN user (e.g., SETUP)
	Signal from/to the analog user (off-hook, hook-flash, ringing)
	Application or removal of tone to the LEA on the call content channel (e.g., C-Tone)
	Application a tone to the user (e.g., ringback tone)
	User A is on-hook
	User A is off-hook
	Subject S and User A are in communication with each other. .
	CCC without the call content.
	CCC with the call content.

Intra-office terminating call to an intercept subject (analog)



Terminating Call to an Intercept Subject (ISDN)

